Extract ATA passwords from a hard disk

After a long wait, here is a new guide that will help anyone who, for fun or profit, wants to retrieve the user / master ATA password that, when activated, protects (but not too much) access to the disk.

I will not bother you with a page of disclaimer text. But do not come and try to find out if you smell burnt electronics or the precious photos of your marriage have been replaced by **zeros.**

CREDITS:

This guide was made thanks to the information found on this Thread found on the HDDGURU forum

Requirements:

Hardware

- A computer with 3.5 "disk drives (the hardest thing to find)
- A floppy disk on which to install the software
- The hard drive to unlock.

Software

- MHDD v. 4.5 in floppy self-extract image available here
- The modified MHDD.zip file with scripts for WD disks taken from the hddguru forum: Mhdd.zip
- The Victoria software, available on Hiren's Boot CD

This procedure is specific to a 120Gb HD **Western Digital** Scorpio and should work on other models produced by Western Digital.

According to ATA specifications, published by t13.org whose last revisions are available in pdf format here , passwords are stored in Host Protected Area (HPA). This part of the disc contains part (or all, depends on the manufacturers) of the disk firmware and is protected by access. The operating system is unable to see this area because the BIOS, which access disk media, protects it.

But the exact location where to find passwords within the HPA depends on the manufacturer. The following procedure is to retrieve the information required for the aforementioned WD Scorpio and most likely for various Western Digital models. Other manufacturers write passwords in different areas and the scripts used contain WD disk offsets.

Let's proceed with the unlock operation ...

Let's start by preparing a floppy disk with MHDD 4.5. Double-clicking on the executable that you should have downloaded (hey, it was in the requirements!) Will create a bootable floppy with the

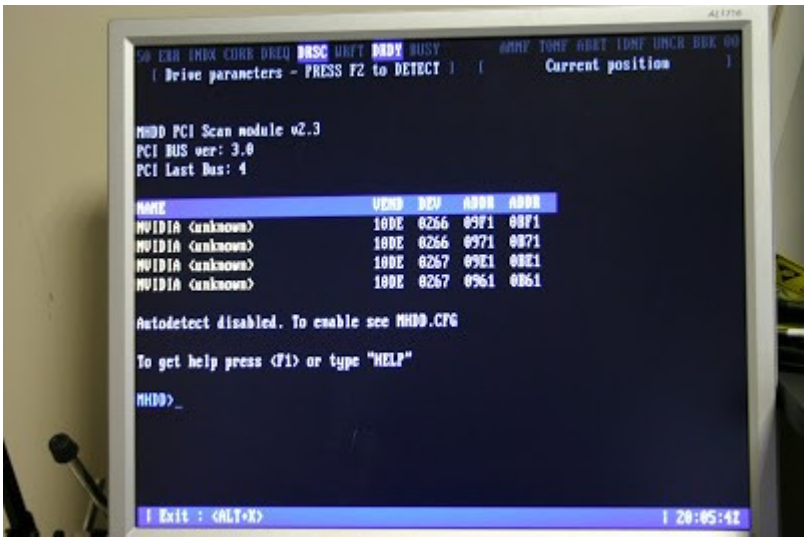
software.
Version 4.5 is used because 4.6 does not have the ATA Terminal that lets you run scripts.

The floppy created replaces the Mhdd.zip with what you have safely downloaded. This file contains the scripts and other files needed to read the protected area.

Now connect the hard disk **DIRECTLY** to a P-ATA / S-ATA port on your **motherboard** . You can not use USB adapters, write blockers, or other interfaces. MHDD bypasses the BIOS and goes read and write directly to the controller. The software works even if the disc is not seen from BIOS!
From the MHDD documentation:

> Just look at this. This is a typical diagram how generic DOS program talks to the drive.
>
> ```
> PROGRAM <---> MSDOS <---> BIOS <---> IDE / SATA Controller <---> Hard Drive
> ```
>
> And now how MHDD works:
>
> ```
> MHDD <---> IDE / SATA controller <---> Hard disk
> ```

Then the computer starts with the floppy diskette. If you look at the autoexec you will notice that a RAMDRIVE is created in which there is the MHDD executable and all the configuration files. This is something to keep in mind, because the dump will be written on the Ramdrive and will then be copied to the physical device A:
I do not go too far in the DOS commands. Be aware, however, that the mouse with this software is only useful as a sticker. You MUST USE KEYBOARD and interact with MS-DOS. A guide to DOS is out of the scope of this document. Do not ask me how to copy a file. I would treat you very badly.



MHDD startup screen (ask to come, but screenshots in DOS did not know how else to do them)

With the [SHIFT + F3] command, the software scans the controller for disk searches

The disk we are interested in is number 12.

The EID command returns the extended disk information

The hard drive is blocked by ATA password and the security level is set to HIGH

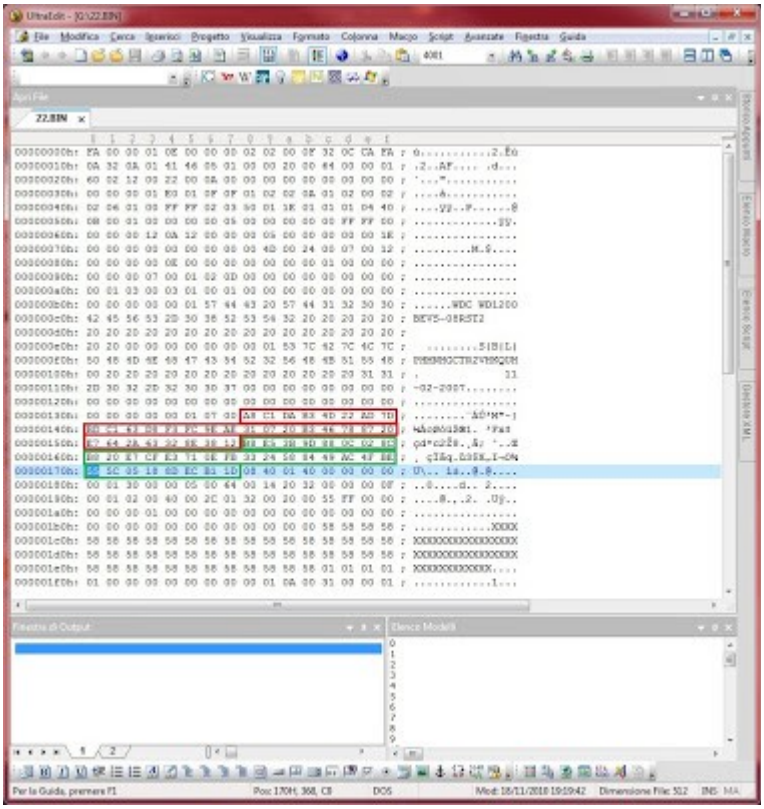
I run the DUMP script with the .dump command (look at the point!)

I do not quite understand the meaning of the hexadecimal values on the REGS rows, however they are specific to Western Digital disks and I think they are related to the offsets needed to read the portion of HPA where the password is kept. You will surely find information on the scrapbooks by enclosing the 409 pages of the ATA specification document ...

The script generates two files: 21.bin and 22.bin.

With the EXIT command we leave the program. The file is now on C: \ MHDD. We copy it onto the diskette and import it into a hex editor.

The 22.bin file imported to UltraEdit:



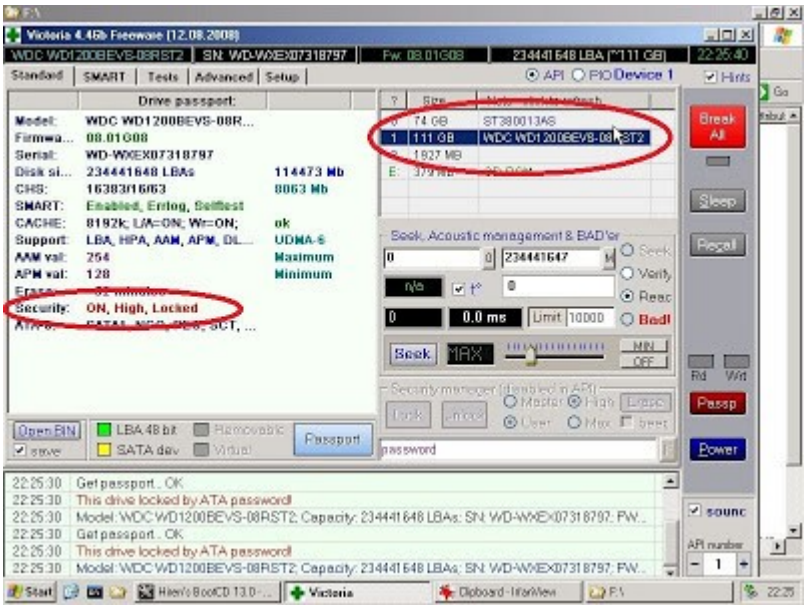
Offsets may be different, but the byte sequence within the file is similar.
At 0x137 offset, the value 07 indicates the ATA security level (in this case HIGH). Passwords are the two 32 bytes highlighted fields. Red is highlighted in the user password. Green password master.

I select the two passwords and from UltraEdit File -> Save Selection by saving the two precious passwords on the USB stick.

Finally you can go back to using the mouse !!!
At the location where we have the hard drive to unlock, we launch Hiren's BootCD in Mini widnows XP mode (I used version 13) and insert the USB stick with the password files.

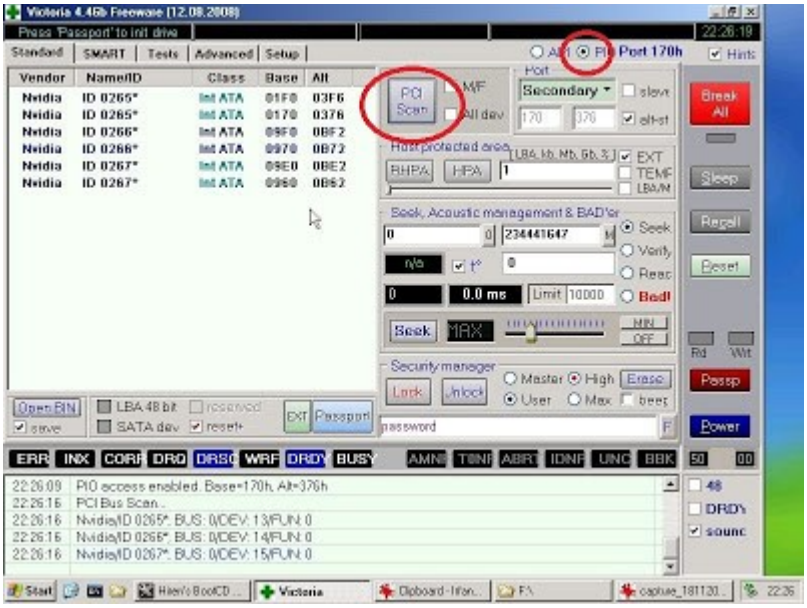
We mount the USB key with Mount Removable Devices on Hiren's desktop.
If you do not install it click on the icon immediately above (Install All Hardware)

From Hiren's menu we launch HBCD -> Hard Disk / Storage -> Victoria

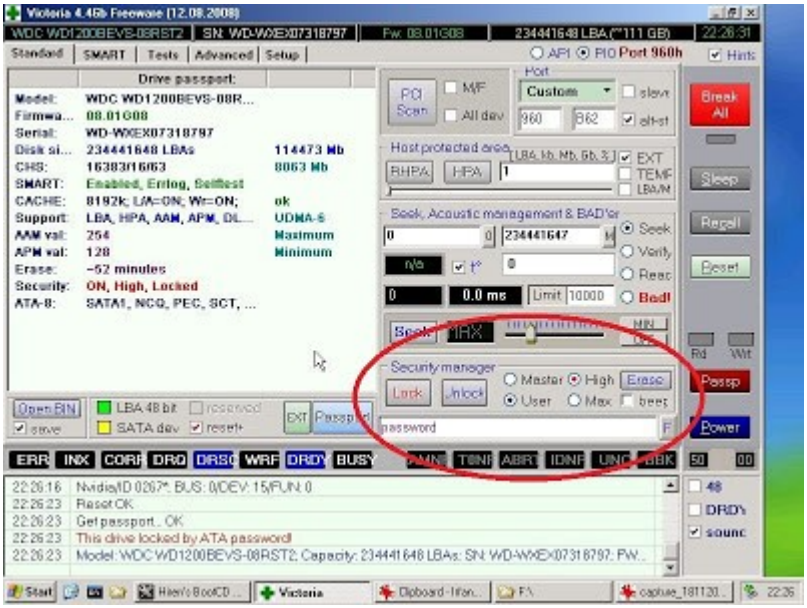


We highlight the disk that interests us and the software tells us it is (still) locked.

However, the Security Manager section can not be used.
Victoria works in two modes: API and PIO. ATA commands (such as lock / unlock) must be sent directly to the controller without BIOS or API mediation. We then go to PIO mode and click on PCI SCAN



And the computer's PATA / SATA ports appear.
Which gate is connected to our target disk?
If we click on each of those ports, the PIO logs are turned on / off at the bottom. Our disk is definitely among those who have the DRDY (Drive Ready) flag switched on.
Double-clicking on the left rows displays a disc that is connected to that port.
In my case, the disc is connected to the port identified by address 0960 .



The disk information is re-released this time, the Security Manager section is active.

Finally here we are. The disc is about to be unlocked ...

Click on F , select the file with our user password (in my case fw1), verify that the radio buttons are set to User and High, we click on Unlock and the file log below will signal the successful outcome of the operation!

If we go back to API mode, the software will continue to signal the disk as locked. Disc mode on the API mode does not update disk status. You just need to turn off your computer and the disc will be unlocked after the next restart.

This solution is not the best, nor what I feel to recommend to the weak in heart. The programs used are EXTREMELY dangerous if not used with care, you may find yourself with an empty or even unusable disk. I recommend.

There are other solutions, such as dedicated hardware or sites that perform remote unlocking. Google is your friend.